

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:)
Schneider et al.)
Serial No.: 10/600,029) Group Art Unit: 2136
Filed: June 20, 2003) Examiner: M. Reza
For: System And Method For Establishing) **Board of Patent Appeals and**
Authenticated Wireless Connection) **Interferences**
Between Mobile Unit And Host)
Confirmation: 6538)

Mail Stop: Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

In support of the Notice of Appeal filed on September 30, 2008, and pursuant to 37 C.F.R. § 41.37, Appellants presents this appeal brief in the above-captioned application.

This is an appeal to the Board of Patent Appeals and Interferences from the Examiner's final rejection of claims 1-29 in the Final Office Action dated on July 17, 2008. The appealed claims are set forth in the attached Claims Appendix.

1. Real Party in Interest

This application is assigned to Symbol Technologies, Inc., a subsidiary of Motorola, Inc., the real party in interest.

2. Related Appeals and Interferences

There are no other appeals or interferences which would directly affect, be directly affected by, or have a bearing on the instant appeal.

3. Status of the Claims

Claims 1-29 stand rejected in the Final Office Action. Therefore, the final rejection of claims 1-29 is being appealed.

4. Status of Amendments

All amendments submitted by the Appellant have been entered. No amendments were filed subsequent to the final rejection.

5. Summary of Claimed Subject Matter

The present invention, as exemplified in claim 1, is directed to a method for establishing an authenticated wireless communication between a first mobile device 2 and a second device 12. (Figure 2; specification at paragraph [0013]) (reference is to the published version). The method involves sending (step 20) an initial signal by the first device 2 to establish a wireless communication with the second device 12, the first device including only a data capturing arrangement ("DCA") 4 as an input device interface with a user thereof. (Figures 1 and 2; specification at paragraphs [0010] and [0012]). The method further involves initiating (step 22) an authentication process by the second device 12. (Figure 2; paragraph [0014]). The method further involves obtaining a PIN code from the user via the DCA (step 26), the PIN code identifying at least one device with which the first device is authorized to communicate. (Figures 1 and 2; paragraphs [0014] and [0016]). The method further involves performing a pairing process (step 28) to compare the PIN code to entries in a database of authorized PIN codes. (Figure 2; paragraph [0018]). According to the method, when the pairing process has been successfully completed, a link key is generated (step 30) to establish the authenticated wireless

communication between the first and second devices. (Id.).

The present invention, as exemplified in claim 13, is directed to a system 1 for establishing an authenticated wireless communication. (Figure 1; paragraph [0009]). The system includes a first wireless mobile device 2 including only a data capturing arrangement ("DCA") 4 as an input device interface with a user thereof (Figure 1; paragraph [0010]). The system 1 further includes a second device 12 receiving an initial signal from the first device 2 to establish a wireless communication, the second device initiating an authentication process. (Figures 1 and 2; paragraphs [0013] and [0014]). In the system 1, the first device 2 obtains a PIN code from the user via the DCA 4, the PIN code identifying at least one device with which the first device 2 is authorized to communicate. (Figure 2; paragraph [0014]). The first and second devices 2, 12 perform a pairing process to compare the PIN code to entries in a database of authorized PIN codes. (Figure 2; paragraph [0018]). When the pairing process has been successfully completed, the first and second devices 2, 12 generate a link key to establish the authenticated wireless communication. (Figure 2; paragraph [0018]).

The present invention, as exemplified in claim 24 is directed to a wireless mobile device 2 for establishing an authenticated wireless communication with a further device 12. (Figure 1; paragraph [0009]). The wireless device 2 includes a processor, a wireless communication arrangement, and a data capturing arrangement ("DCA") 4, with the DCA 4 being the only input device interface for a user thereof. (Figure 1; paragraph [0010]). The processor generates a request for establishing an authenticated wireless communication. (Paragraph [0013]). The request is forwarded to the further device 12 via the communication arrangement, the communication arrangement receiving from the further device 12 a first sample data, compiled from a collection of random data, and a request for second data. (Paragraph [0018]). The DCA obtains a PIN code from the user, the PIN code identifying at least one device with which the mobile device is authorized to communicate. (Paragraph [0015]). The processor generates the second data as a function of the PIN code, the first sample data and the hashing procedure, the second data being provided, by the mobile device, to the further device. (Paragraph [0018]). The further device 12 generates third data as a function of at least one of the authorized PIN codes stored in a database, the second data received from the mobile device and the hashing procedure.

(*Id.*). When the second data received from the mobile device 2 matches to the third data, the mobile device 2 and the further device 12 generate a link key to establish the authenticated wireless communication. (Paragraph [0020]).

6. Grounds of Rejection to be Reviewed on Appeal

- I. Whether claims 1-29 are unpatentable under 35 U.S.C. § 103(a) over U.S. Published Appln. No. 2003/0172283 to O'Hara ("O'Hara") in view of U.S. Patent No. 5,534,857 to Laing ("Laing").

7. Argument

Claim 1, recites, in relevant portion: "[a] method for establishing an authenticated wireless communication between a first mobile device and a second device, comprising the steps of:... sending an initial signal by the first device to establish a wireless communication with the second device, the first device including only a data capturing arrangement ("DCA") as an input device interface with a user thereof... obtaining a PIN code from the user via the DCA, the PIN code identifying at least one device with which the first device is authorized to communicate; performing a pairing process to compare the PIN code to entries in a database of authorized PIN codes; when the pairing process has been successfully completed, generating a link key to establish the authenticated wireless communication between the first and second devices."

The Examiner asserts that O'Hara teaches a device that "include[es] only a data capturing arrangement ("DCA") as an input device interface with a user thereof." This language means that the DCA is the only input device in the first device. That is untrue of the O'Hara device because, as shown in Figures 1 and 2, it includes a keypad, a touchscreen, and a biometric scanner. Therefore, O'Hara fails to meet this particular limitation, and Laing does not cure this deficiency. The Examiner also asserts that O'Hara teaches obtaining a PIN code that identifies the devices authorized to communicate with the first device. The Examiner appears to believe that the biometric data obtained by the O'Hara device meets the PIN limitation of the claim. This is incorrect. The term PIN is not intended to cover any information that can uniquely identify something else. The term PIN covers numeric information, not the physical traits of a person,

however unique such traits may be. Therefore, O'Hara does not teach the use of PIN. Laing does not cure this deficiency. Accordingly, withdrawal of this rejection is requested.

In the Advisory Action, the Examiner appears determined to ignore the ordinary meaning of "only." Indeed, the Examiner goes so far as to say that the argument of the Appellants are "totally irrelevant." The justification for this "total" irrelevance appears confused, since the Examiner does not deny that O'Hara has more than one data capturing arrangement, but yet insists that this does not preclude O'Hara from meeting the above-discussed claim language. Apparently, the Examiner hinges his argument on the following statement : "When some device has a scanner with other input facilities it obviously discloses the idea that some device could have only a scanner excluded other input." Of course, the Examiner cannot find any support in O'Hara for a device with only a data capturing arrangement as the input arrangement for the device. The argument, then, is bottomed on the unsupported assertion that of course one of ordinary skill in the art could have eliminated all the input devices in O'Hara but one. No support in the prior art exists for this assertion.

The Examiner also asserts that "although O'HARA's device has other input peripheral for capturing the biometric information it only uses the scanner input. Thus it discloses the only data capturing device." This is nothing but sophistry, since it is an argument that is contrary to the common understanding of "only." If a claim recites a device having only one input arrangement, and the prior art has input arrangement A and B, then by any rational standard for judging the meaning of the English language, the prior art can not be said to meet the claim. Moreover, as to the Examiner's statement that the "only" feature of the claims "is not an invention at all," it is not the role of the Examiner to condescend to the inventors on what is or is not an invention. Rather than engage in such unnecessary editorializing, the Examiner would do well instead to confine himself to his statutory role, namely, to achieve an understanding of the claims based on a common sense understanding of the language, gather the evidence believed to be relevant based on that understanding, and apply the evidence to the claims.

Serial No.: 10/600,029

Group Art Unit: 2136

Attorney Docket No.: 40116 - 03701

8. Conclusion

For the reasons set forth above, Appellants respectfully request that the Board reverse the final rejections of the claims by the Examiner under 35 U.S.C. § 103(a) and indicate that claims 1-29 are allowable.

Respectfully submitted,

Date: October 30, 2008



By: _____
Oleg F. Kaplun (Reg. No. 45,559)

Fay Kaplun & Marcin, LLP
150 Broadway, Suite 702
New York, NY 10038
Tel: (212) 619-6000
Fax: (212) 619-0276

CLAIMS APPENDIX

1. (Previously Presented) A method for establishing an authenticated wireless communication between a first mobile device and a second device, comprising the steps of:

 sending an initial signal by the first device to establish a wireless communication with the second device, the first device including only a data capturing arrangement ("DCA") as an input device interface with a user thereof;

 initiating an authentication process by the second device;

 obtaining a PIN code from the user via the DCA, the PIN code identifying at least one device with which the first device is authorized to communicate;

 performing a pairing process to compare the PIN code to entries in a database of authorized PIN codes;

 when the pairing process has been successfully completed, generating a link key to establish the authenticated wireless communication between the first and second devices.

2. (Original) The method according to claim 1, wherein the databases is stored in a memory arrangement of the second device.

3. (Original) The method according to claim 1, wherein the first device is a mobile barcode scanner.

4. (Original) The method according to claim 1, wherein the first device communicates with the second device using Bluetooth technology.

5. (Original) The method according to claim 1, wherein the obtaining step further includes the following substeps:

 scanning a barcode using the DCA, the barcode being provided by the user as the PIN code, and

 converting the barcode into the PIN code using a processor of the first device.

6. (Original) The method according to claim 1, wherein the second device includes a wireless access point which communicates with the first device.

7. (Original) The method according to claim 1, wherein the first device includes an alerting arrangement notifying the user when to enter the PIN code.

8. (Original) The method according to claim 7, wherein the alerting arrangement includes at least one of a speaker emitting a predetermined sound and a set of LEDs emitting a predetermined lighting pattern.

9. (Original) The method according to claim 1, wherein the obtaining step includes the following substeps:

limiting a time period for the user to enter the PIN code to a predetermined time period, and

refusing to accept the PIN code from the user when the predetermined time period has expired.

10. (Previously Presented) The method according to claim 1, wherein the pairing process includes the following substeps:

compiling a first sample data, from a collection of random data, by the second device, the second device then providing the first sample data to the first device,

generating second data, by the first device, as a function of the first sample data, the PIN code and a hashing procedure;

providing at least a portion of the second data by the first device to the second device,

generating third data by the second device as a function of at least one of the authorized PIN codes stored in the database, the second data received from the first device and the hashing procedure;

comparing, by the second device, the second data received from the first device to the corresponding third data, and

when the second data received from the first device matches to the third data, generating an indication the pairing process is successfully completed.

11. (Original) The method according to claim 1, wherein the link key is one of a temporary key which is effective only for a single session and a long-term key which is effective for multiple

sessions between the first and second devices.

12. (Original) The method according to claim 1, further comprising the step of:
establishing a secure communication between the first and second devices using a predetermined encryption technology.
13. (Previously Presented) A system for establishing an authenticated wireless communication, comprising:
 - a first wireless mobile device including only a data capturing arrangement (“DCA”) as an input device interface with a user thereof; and
 - a second device receiving an initial signal from the first device to establish a wireless communication, the second device initiating an authentication process,
wherein the first device obtains a PIN code from the user via the DCA, the PIN code identifying at least one device with which the first device is authorized to communicate, wherein the first and second devices perform a pairing process to compare the PIN code to entries in a database of authorized PIN codes, and wherein, when the pairing process has been successfully completed, the first and second devices generate a link key to establish the authenticated wireless communication.
14. (Original) The system according to claim 13, wherein the second device includes a memory arrangement storing the database.
15. (Original) The system according to claim 13, wherein the first device is a mobile barcode scanner.
16. (Original) The system according to claim 13, wherein the first device communicates with the second device using Bluetooth technology.
17. (Original) The system according to claim 13, wherein the first device scans a barcode using the DCA, the barcode being provided by the user as the PIN code, a processor of the first device converting the barcode into the PIN code.

18. (Original) The system according to claim 13, wherein the second device includes a wireless access point which communicates with the first device.

19. (Original) The system according to claim 13, wherein the first device includes an alerting arrangement notifying the user to enter the PIN code.

20. (Original) The system according to claim 19, wherein the alerting arrangement includes at least one of a speaker emitting a predetermined sound and a set of LEDs emitting a light in a predetermined lighting patterns.

21. (Previously Presented) The system according to claim 13, wherein the pairing process includes the following substeps:

compiling a first sample data, from a collection of random data, by the second device, the second device then providing the first sample data to the first device,

generating second data, by the first device, as a function of the first sample data, the PIN code and a hashing procedure;

providing at least a portion of the second data by the first device to the second device,

generating third data by the second device as a function of at least one of the authorized PIN codes stored in the database, the second data received from the first device and the hashing procedure;

comparing, by the second device, the second data received from the first device to the corresponding third data, and

when the second data received from the first device matches to the third data, generating an indication the pairing process is successfully completed.

22. (Original) The system according to claim 15, wherein the link key is one of a temporary key which is effective only for a single session and a long-term key which is effective for multiple sessions between the first and second devices.

23. (Original) The system according to claim 13, wherein the first and second devices establish a secure communication using a predetermined encryption technology.

24. (Previously Presented) A wireless mobile device for establishing an authenticated wireless communication with a further device, comprising:

a processor;

a wireless communication arrangement; and

a data capturing arrangement (“DCA”) being the only input device interface for a user thereof,

wherein the processor generates a request for establishing an authenticated wireless communication, the request being forwarded to the further device via the communication arrangement, the communication arrangement receives from the further device a first sample data, compiled from a collection of random data, and a request for second data, the DCA obtaining a PIN code from the user, the PIN code identifying at least one device with which the mobile device is authorized to communicate, the processor generating the second data as a function of the PIN code, the first sample data and the hashing procedure, the second data being provided, by the mobile device, to the further device,

wherein the further device generates third data as a function of at least one of the authorized PIN codes stored in a database, the second data received from the mobile device and the hashing procedure, and

wherein, when the second data received from the mobile device matches to the third data, the mobile device and the further device generate a link key to establish the authenticated wireless communication.

25. (Previously Presented) The mobile device according to claim 24, wherein the mobile device is a mobile barcode scanner.

26. (Previously Presented) The mobile device according to claim 24, wherein the mobile device communicates with the further device using Bluetooth technology.

27. (Previously Presented) The mobile device according to claim 24, wherein the DCA scans a barcode which is provided by the user as the PIN code, the processor converting the barcode into the PIN code.

Serial No.: 10/600,029

Group Art Unit: 2136

Attorney Docket No.: 40116 - 03701

28. (Previously Presented) The mobile device according to claim 24, further comprising:
an alerting arrangement notifying the user to enter the PIN code.
29. (Previously Presented) The mobile device according to claim 24, wherein the alerting arrangement includes at least one of a speaker emitting a predetermined sound and a set of LEDs emitting a predetermined lighting pattern.

Serial No.: 10/600,029

Group Art Unit: 2136

Attorney Docket No.: 40116 - 03701

EVIDENCE APPENDIX

No evidence has been entered or relied upon in the present appeal.

Serial No.: 10/600,029

Group Art Unit: 2136

Attorney Docket No.: 40116 - 03701

RELATED PROCEEDING APPENDIX

No decisions have been rendered regarding the present appeal or any proceedings related thereto.